AVRUPA BİRLİĞİ VERİ KORUMA DİREKTİFİ EKSENİNDE HASSAS (KİŞİSEL) VERİLER VE İŞLENMESİ

Doç. Dr. Cemil Kaya*

GİRİŞ

Bilişim teknolojilerinin hızla gelişmesi kişisel verilerin işlenmesini kaçınılmaz kılmaktadır. Kişisel verilerin işlenmesi ise bu verilerin elde edilmesi ile başlayan ve kaydedilmesi, düzenlenmesi, uyarlanması, değiştirilmesi, düzeltilmesi, incelenmesi, kullanılması, açıklanması, sıralanması, birleştirilmesi ve silinmesi ile devam eden bir süreci ifade etmektedir. Bireyleri yakından ilgilendiren bütün bu süreçlerin onların temel hak ve özgürlüklerini ve özellikle de özel yaşamlarının dokunulmazlığı haklarını güvence altına almak açısından kanuni bir düzenlemeye tabi tutulması gerekmektedir. İşte bu amaçla veri koruma kanunları kabul edilmektedir[1].

Veri koruma kanunlarında düzenleme altına alman nazik bir konu ise "hassas veriler ve bu verilerin işlenmesi"dir. Veri koruma kanunları bulunan hemen hemen bütün ülkeler hassasiyet gösteren bazı veri türleri olduğunu kabul etmişler ve bu yönde düzenlemeler yapmışlardır. Hatta hassas verilerin veri koruma kanunlarının kalbinde bulunduğu bazı yazarlarca ifade edilmiştir[2]. Veri koruma kanunları ile hassas veriler, özellikli ve kapsamlı bir koruma altına alınmaya çalışılmaktadır. Bu amaçla veri koruma kanunlarında hangi tür verilerin hassas veri sayılacağı ve bunların hangi istisnai haller altında işleneceği belirlenmektedir. Kısacası hassas veriler özel bir rejime tabi tutulmaktadır. Veri koruma kanunları ile genellikle kişilerin ırksal kökenine, dini inançlarına, sağlık durumu ve siyasi görüşlerine ilişkin veriler hassas veri olarak kabul edilmektedir. Veri sahibinin açık muvafakatının bulunması ve yaşamsal çıkarlarının korunması halleri ise hassas verilerin işlenmesinde temel istisnalar arasında yer almaktadır.

---

* İstanbul Üniversitesi Hukuk Fakültesi İdare Hukuku Anabilim Dalı Öğretim Üyesi

[1] Hatta bu kanunların oldukça ayrıntılı hükümler içerdiği görülmektedir. Örneğin, 1997 tarihli Polonya Kişisel Verilerin Korunması Hakkında Kanun'un 9. maddesinde Veri Koruma Otoriteleri üyelerinin edecekleri yemin metni dahi bu Kanunda gösterilmiştir. Bkz. http://ec.europa.eu/justice_home/fsj/privacy/docs/implementation/poland_en.pdf (20.03.2010)

[2] **Lloyd**, Ian J., Information Technology Law, Fifth Edition, Oxford University Press, Oxford 2008, s. 42.

Veri koruma kanunları yanında hassas veriler, Avrupa Konseyinin 28 Ocak 1981 tarih ve 108 sayılı "Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına Dair Sözleşmesi"nin 6. maddesinde[3] ve "Kişisel Verilerin İşlenmesi ve Bu Verilerin Transferi Konusunda Bireylerin Korunması Hakkında Avrupa Birliği Direktifi"nin 8. maddesinde[4] özel koruma altına alınmıştır.

İşte bu makalede Veri Koruma Direktifi ekseninde hassas (kişisel) veriler ve bu verilerin işlenebileceği haller ele alınacaktır.

I. HASSAS VERİLER

A. Tanım ve Kavram Sorunu

Hassas (duyarlı) veriler, kişisel verilerin daha fazla koruma uygulanan küçük bir grubu olarak tanımlanabilir[5]. Veri Koruma Direktifi'nin giriş kısmında ise hassas veriler, temel hakları ve özel yaşamın gizliliğini ihlal edici yapıda bulunan veriler olarak tanımlanmaktadır[6]. Hassas veriler, kapsamına giren türler yoluyla da tanımlanabilir. Buna göre doğrudan veya dolaylı olarak kişilerin ırki ve etnik kökeni, ten rengini, siyasi görüşlerini, dini ve felsefi inançlarını, sendika üyeliğini, sağlık ve cinsel yaşamını ve mahkumiyetlerini ortaya çıkaran verilere hassas veri adı verilir.

Diğer taraftan, hassas verileri ifade etmek üzere kullanılan kavramlarda bir birliktelik olmadığı da görülmektedir. Bu tür verileri ifade etmek üzere veri koruma kanunlarında genellikle "hassas veri" (*sensitive data*) kavramı kullanılmakla birlikte "özel kategorili kişisel veriler" (*special categories of personal data – besondere arten personenbezogener daten*)[7], "özel kişisel veriler" (*special personal data*)[8] ve hatta "özel korumaya layık olan veriler" (*data deserving special protection – besonders schutzwürdige daten*)[9] kavramları da

---

[3] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Bundan sonra 108 sayılı Sözleşme olarak anılacaktır.

[4] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. OJ L 281, 23.11.1995, p. 31–50. Bundan sonra Veri Koruma Direktifi olarak anılacaktır.

[5] **Carey**, Peter, Data Protection: A Practical Guide to UK and EU Law, Third Edition, Oxford University Pres, Oxford 2009, s. 81.

[6] Direktif, Recital 33.

[7] Örnek olarak bkz. 2001 tarihli Alman Federal Veri Koruma Kanunu m. 3/9. http://www.bfdi.bund.de/cae/servlet/contentblob/844438/publicationFile/51362/aktualisiertesBDSG.pdf (20.03.2010); 2003 tarihli Litvanya Kişisel Verilerin Hukuki Korunması Hakkında Kanun m. 2/9. http://www.ada.lt/ images/cms/ File/ pers.data.prot.law.pdf (20.03.2010); 2002 tarihli Slovakya Kişisel Verileri Koruma Hakkında Kanun m. 8. http://ec.europa.eu/ justice_home/ fsj/privacy/docs/ implementation/ slovakia_428_02_en.pdf (20.03.2010);

[8] Örnek olarak bkz. 2000 tarihli Hollanda Veri Koruma Kanunu m. 16. http://www.dutchdpa.nl/ downloads_wetten/wbp.pdf (20.03.2010)

[9] Örnek olarak bkz. 2000 tarihli Avusturya Federal Kişisel Verilerin Korunması İle İlgili Kanun m. 4/2. http://www.dsk.gv.at/site/6230/default.aspx (20.03.2010)

kullanılmaktadır. Bu makalede ise en yaygın kullanım şekline sahip olan "hassas veri" kavramı tercih edilecektir.

B. Hassas Veri Türleri

Veri Koruma Direktifi'nin 8. maddesinin 1. fıkrasında,

1) Irksal ve etnik kökene,

2) Siyasi görüşlere[10],

3) Dini ve felsefi inançlara,

4) Sendika üyeliğine,

5) Sağlık durumuna ve cinsel yaşama,

ilişkin veriler hassas veri olarak kabul edilmiştir.

Hassas veriler bu fıkrada sınırlı sayıda (*exhaustive*) sayılmakla beraber aynı maddenin 5. fıkrası uyarınca suçlar, mahkumiyetler ve güvenlik tedbirleri ile ilgili verilerin de bu nitelikte olduğu söylenebilir.

Diğer taraftan 108 sayılı Sözleşme'nin 6. maddesinde ise ırksal kökene, siyasi görüşlere, dini ve diğer inançlara, sağlığa ve cinsel yaşama ve mahkumiyetlere ilişkin veriler hassas veri olarak kabul edilmiştir.

Veri koruma kanunlarına sahip olan bütün ülkelerde de hemen hemen bu nitelikteki veriler hassas veri olarak kabul edilmiştir. Ancak bunlardan farklı olarak genetik bilgilere (Polonya, İzlanda, Estonya ve Bulgaristan), biometrik bilgilere (Slovenya[11], Slovakya, Çek Cumhuriyeti), ten rengine (İzlanda), milli kökene (Çek Cumhuriyeti ve Slovenya), siyasi partilere veya hareketlere (Slovakya), dernek üyeliğine (İtalya), özür durumuna (Estonya), bağımlılıklara (Polonya), alkol, tıbbi ilaç ve uyuşturucu kullanımına (İzlanda), cinsel yaşama ve cinsel davranışlara (İzlanda), cinsel tercihlere ve cinsel yaşama (Finlandiya), sosyal görüşlere (Finlandiya), sağlık, hastalık veya handikap (özür) durumuna ve tedavi ve diğer benzer tedbirlere (Finlandiya), sosyal refah ihtiyaçlarına ve alman yararlanmalara, destek ve diğer sosyal refah yardımlarına (Finlandiya), fiziksel ve zihinsel sağlık ve duruma (İngiltere), işlenilen ya da işlendiği iddia edilen suçlara (İngiltere), işlenilen ya da işlendiği iddia edilen suçlar için yürütülen kovuşturmalara, bu kovuşturulmaların sonlandırılmasma ve bu kovuşturmalar sonucunda bir mahkeme tarafından verilen mahkumiyetlere (İngiltere) ilişkin veriler de veri koruma kanunlarında hassas veri olarak

---

[10] Bu kavram 1992 tarihli İsviçre Federal Veri Koruma Kanunu'nda "ideolojik görüş ve faaliyetler" şeklinde formülize edilmiştir. Bkz. http://www.admin.eh/ch/e/rs/2/235.1.en.pdf (20.03.2010).

[11] 2004 tarihli Slovenya Kişisel Veri Koruma Kanunu'nda biometrik veriler şöyle tanımlanmıştır (m. 6/21): Biometrik özellikler, bütün bireylerin sahip olduğu fiziksel, fizyolojik ve davranışsal özelliklerdir. Fakat bu özellikler spesifik olarak her bir bireye özgüdür ve daimidir. Bunlar, özellikle, parmak izi kullanımı, parmağın papiler çizgilerini kaydetme, iris taraması, retinal tarama, yüz ile ilgili özellikleri kaydetme, bir kulağı kaydetme, DNA taraması ve yürüme özelliği yoluyla bir bireyi belirlemek için kullanılabilir. http://ec.europa.eu/justice_home/fsj/privacy/docs/implementation/personal_data_protection_act_rs_2004.pdf (20.03.2010)

kabul edilmiştir[12]. Görüldüğü gibi AB ülkelerinin hassas veri türlerinde önemli farklılıklar bulunmaktadır.

Son yıllarda kabul edilen veri koruma kanunlarında "genetik bilgiler" ve "biometrik bilgiler"in, sağlığa ilişkin verilerden ayrı olarak hassas veriler arasında sayıldığı dikkat çekmektedir. Genetik veriler ve biometrik verilerin bireylerin sağlığa ilişkin verileri içinde yer aldığı konusunda görüşler bulunmakla birlikte, veri koruma uzmanları, tartışmalara mahal bırakmamak açısından, giderek artan şekilde günlük yaşantımızı etkileyen[13] genetik veriler ve biometrik verilerin hassas veriler arasında ismen sayılmalarının daha faydalı olacağını ileri sürmektedir[14].

1992 tarihli İsviçre Federal Veri Koruma Kanunu'nda hassas veriler, Veri Koruma Direktifi'nden ve diğer ülkelerin veri koruma kanunlarından oldukça farklı şekilde formülize edilmiştir (m. 3/c)[15]. Bunlar, 1) Dini, ideolojik, siyasi ve sendika ile bağlantılı görüş ve faaliyetlere, 2) Sağlık, mahrem alan (*the intimate sphere*) ve ırksal kökene, 3) Sosyal güvenlik tedbirlerine/dosyalarına, 4) İdari ve cezai prosedür ve yaptırımlara, ilişkin verilerdir.

2003 tarihli İtalyan Kişisel Veri Koruma Kodu, bugün itibarıyla, AB ülkeleri arasında en ayrıntılı veri koruma kanunudur. Hatta diğer ülke kanunlarından farklı olarak İtalyan Kodu'nda aslında bir hassas veri türü olan yargılamaya ait veriler (*judicial data*) hassas verilerden ayrı şekilde özel olarak düzenlenmiştir (m. 4)[16].

Bazı ülkelerin veri koruma kanunlarında ise "özel kişisel veri" ve "hassas kişisel veri" ayrımı da yapılmaktadır. Örneğin, 2003 tarihli Estonya Kişisel Veri Koruma Kanunu'nda şu veriler hassas kişisel veri değil ama özel kişisel veri olarak kabul edilmiştir (m. 4/2-4)[17]: 1) Aile yaşamına, 2) Sosyal yardım ve sosyal hizmet almak için yapılan müracaatlara, 3) Maruz kalman zihinsel ve fiziksel acılara, 4) Vergi borçları ile ilgili veriler hariç vergileme işlemi sırasında bir kişi hakkında toplanan verilere, ait bilgiler.

Diğer taraftan yapılan anketler kanun koyucunun hassas veri algılaması ile bireylerin hassas veri algılamasının farklı olduğunu da ortaya koymuştur. İngiltere'de 2006 yılında Bilgi Görevlisi (*Information Commissioner*) adına yapılan bir anket bireylerin hangi tür bilgileri hassas veri olarak gördüklerini ortaya koyması açısından dikkat çekicidir. İlginç şekilde, Veri Koruma Direktifi'nde ve veri koruma kanunlarının hemen hemen hepsinde hassas veriler arasında dahi

---

[12] http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm (20.03.2010)

[13] Mart 2005'te Avrupa Komisyonu biometrikler hakkında kapsamlı bir çalışma yayımlamıştır. Bu çalışmada, 2006 yılından itibaren biometriklerin pasaportlarda, vize müracaatlarında ve ikamet izinlerinde kullanılması kararının ardından bunların nasıl günlük yaşamı etkileyecekleri gösterilmiştir. Nakleden **Jay**, Rosemary, Data Protection: Law and Practice, Sweet & Maxwell, London 2007, s. 273, dn. 1.

[14] **Jay**, s. 272.

[15] http://www.admin.eh/ch/e/rs/2/235.1.en.pdf (20.03.2010). Buna çok yakın benzer bir düzenleme için bkz. 2002 tarihli Liechtenstein Veri Koruma Kanunu m. 3/e. http://www.llv.li/pdf-llv-dss-dpa-fl_en_2009-11-30.pdf (20.03.2010)

[16] http://www.garanteprivacy.it/garante/document?ID=1219452 (20.03.2010)

[17] http://www.legaltext.ee/text/en/X70030.htm (20.03.2010)

sayılmayan "finansal veriler" ankete katılanlar tarafından en yüksek oranda hassas veri olarak görülmüştür. Anket sonuçları aşağıdaki gibidir[18]:

Veri Türleri	**Yüzdelik Oran**
Finansal Veriler	88.0
Sağlık Bilgileri	72.0
Kişisel İletişim Bilgileri	68.0
Cinsel Yaşam Bilgileri	67.0
Biometrik Bilgiler	63.0
Genetik Bilgiler	63.0
Suç Kayıtları	58.0
Bir Kişinin Ziyaret Ettiği İnternet Sitelerine İlişkin Bilgiler	43.0
Siyasi Düşünceler	42.0
Eğitim Bilgileri	42.0
Irk ve Etnik Köken İle İlgili Veriler	41.0
Çalışma Geçmişi İle İlgili Veriler	41.0
Siyasi Parti/Teşkilat Üyeliği	38.0
Dini ve Felsefi İnançlar	37.0
Sendika Üyeliği	33.0

Amerika'da genel bir veri koruma kanunu *bulunmaması* ve kişisel verilerin açıklanması yönünde ciddi bir baskı oluşturabilecek bilgi edinme hakkı kanunu *bulunmasının* hassas verilerin özel olarak korunmasını olumsuz yönde etkilediği ileri sürülmektedir[19]. Diğer taraftan Amerika'da 1974 tarihli Özel Yaşamın Gizliliği Kanunu (*The Privacy Act*) ve 1966 tarihli Bilgi Edinme Hakkı Kanunu (*The Freedom of Information Act*) hassas veriler için özel bir koruma da getirmektedir. Özel Yaşamın Gizliliği Kanunu tek bir tür hassas veri için özel koruma getirmektedir. Kanun, bireylerin İlk Değişiklik (*the First Amendment*) ile güvence altına alman hakları (özgür konuşma ve dini faaliyetler) kullanmalarını belirleyen kayıtları tutmayı kamu otoritelerine yasaklamaktadır[20]. Yine Bilgi Edinme Hakkı Kanunu hassas veriler için koruma getiren açık bir hüküm içermemekle beraber bu nitelikteki verileri üçüncü kişilere açıklamayı yasaklama anlayışı benimsemiştir. Bu bağlamda Kanunun iki maddesi önemlidir: 1) Özel yaşamın açıkça mazur görülemeyen ihlaline yol açacak "kişisel", "tıbbi" ve "benzer dosyalar" açıklanamaz. 2) Kişisel mahremiyetin mazur görülemeyen ihlaline yol açacağının makul olarak beklenmesi halinde hukukun uygulanması amacıyla derlenmiş kayıt ve bilgiler açıklanamaz[21].

---

[18] 2006 Annual Tracking Report. Nakleden **Lloyd**, s. 42-43.

[19] **Schwartz**, Paul M. / **Reidenberg**, Joel R., Data Privacy Law: A Study of United States Data Protection, Michie Law Publishers, Virginia 1996, s. 140.

[20] The Privacy Act of 1974. 5 U.S.C. § 552a(e)(7). Nakleden **Schwartz / Reidenberg**, s. 112.

[21] The Freedom of Information Act, 5 U.S.C. § 552(b)(6) ve (7). Nakleden **Schwartz / Reidenberg**, s. 112-113.

C. Karşılaşılan Güçlükler

Veri koruma kanunlarında hassas veri türlerini saymak bütün belirsizliklerin bertaraf edildiği anlamına da gelmemektedir. Şöyle ki, hassas veri türleri bazen kolayca örneklendirilebilir[22]: Bir işverenin çalışanlarının sendika üyeliği kaydı; Bir uçak yolcusunun dini inancına uygun yemek tercihini gösteren bilgi; Belirli bir kişi için tekerlekli sandalye erişiminin gerekli olduğunu belirten otel rezervasyon bilgisi; Bir çalışanın apandisit ameliyatı için hastanede olduğunu gösteren kayıt; Bir müşterinin striptiz kulüplerine gitmeyi sevdiğini açıklayan piyasa bilgisi; Bir kişinin uyuşturucu madde bağımlısı olduğunu gösteren hastane kayıtları; Bir kişinin kara para aklama suçunu işlediğini gösteren bilgi.

Diğer taraftan iş bu kadar kolay da değildir. Örneğin, bir işçinin personel dosyasında "işvereninin her bir fırsatta işçilerini sömüren zalim bir kapitalist olduğu" fikrine sahip olduğunu gösteren bir veri siyasi düşünceye mi yoksa problemli bir işçiye mi ilişkin kabul edilecektir?[23]. Yine bir kişinin internette evinin bulunduğu yere yakın bir Babtist Kilise araması halinde internette online araştırma imkanı sunan şirket bu kişi hakkında hassas veri işliyor mu kabul edilecektir?[24]. Pasaportlara biometrik verilerin kaydedilmesi sağlık verilerinin işlenmesi anlamına mı gelmektedir?[25]. Bir kişinin adı-soyadı tek başına hassas veri sayılabilecek midir?[26] Şüphesiz bu soruların cevabını kesin olarak vermek mümkün değildir.

Bu güçlükler mahkemeleri de meşgul etmektedir. İngiltere'de *Naomi Campbell v MGN* davasında Mahkeme, bayan *Campbell*'in fotoğrafları onun ten rengini ortaya çıkarttığı için bunların hassas veri olarak nitelenip nitelenmeyeceğini değerlendirmek zorunda kalmıştır. Mahkeme, fotoğrafların bayan *Campbell*'in ırksal kökeni ile ilgili bilgileri açıkladığına, ancak bu durumun fotoğrafların yayınlanma amacı karşısında önemsiz kaldığına, veri sahibinin, tanınmış siyah bir manken olmaktan gurur duyduğu ve siyah bir kadın olarak fotoğraflarının çekilmesinin onun yaşam tarzının ve mesleğinin bir parçası olduğu hallerde durumun değişeceğine ve bu olayda fotoğrafların hassas veri olarak kabul edilemeyeceğine karar vermiştir[27]. Bununla birlikte aynı davada mahkeme *the Narcotics Anonymous*'de[28] alman tedavinin niteliği ve detayları ile

---

[22] **Carey**, s. 83.

[23] **Jay**, s. 272.

[24] **Carey**, s. 83.

[25] **Carey**, s. 83.

[26] **Singleton**, Susan, Tolley's Data Protection Handbook, 4th Edition, Lexis Nexis Butterworths, London 2006, s. 568.

[27] Campbell v MGN Ltd per Morland J [2002] EWHC 499, (2002) HRLR 28 at paras 85-86. The House of Lords restored the orders of Morland J [2004] 2 AC 457. Nakleden **Macdonald**, John / **Crail**, Ross / **Jones** Clive H., The Law of Freedom of Information, Second Edition, Oxford University Press, Oxfod 2009, s. 355; **Jay**, s. 273; **Carey**, s. 83; **Singleton**, 568-569.

[28] *The Narcotics Anonymous*, İngiltere'de hiçbir ayrım gözetmeden uyuşturucu bağımlılarına yardım amacı taşıyan ve kar amacı gütmeyen gönüllü bir kuruluştur.

ilgili bilgileri, fiziksel ve zihinsel sağlık veya durumla ilgili bilgiler olarak görmüş ve bu nedenle de açıkça hassas veri tanımı içinde mütalaa etmiştir[29].

Avrupa Toplulukları Adalet Divam'mn (*European Court of Justice – ECJ*) (ATAD) *Bodil Lindqvist* kararı da hassas veri kavramını çevreleyen zorlukları gösterme açısından önemlidir. *Bodil Lindqvist* davasında[30] İsveç Mahkemeleri tarafından sorulan bazı sorulara karşılık ATAD'dan "ön karar" (*preliminary ruling*) vermesi istenmiştir. Bu davaya konu olayda Bayan *Lindqvist*, kendi internet sitesinde meslekdaşları hakkında kişisel bilgileri yayımladığı gerekçesiyle İsveç Veri Koruma Kanunu'nu ihlal etmekle suçlanmıştı. Bayan *Lindqvist*, meslekdaşlarmm ad ve soyadlarını ya da sadece adlarını kendi internet sitesine koymuştu. Ayrıca Bayan *Lindqvist*, meslekdaşlarmm yaptıkları işleri, onların hobilerini, aile durumlarını, telefon numaralarını da bu siteye koymuştu. Aynı zamanda bir meslekdaşmın ayağını incittiğini ve bu nedenle de kısmi statüde çalıştığına ilişkin bilgiye de sitesinde yer vermişti[31]. İsveç Makamları, diğerleriyle birlikte, Bayan *Lindqvist*'i, meslekdaşları ile ilgili hassas verileri onların muvafakatını almadan ve İsveç Ulusal Veri Koruma Otoritesinden izin almadan işlemekle suçlamıştı[32]. Acaba bir meslekdaşmın ayağını incittiğine ve bu nedenle de kısmi statüde çalıştığına ilişkin bilgi hassas veri kabul edilebilir miydi? ATAD'm cevabı özlü ve önemli idi: "Direktifin amaçları ışığında, 8. maddenin 1. fıkrasında kullanılan sağlıkla ilgili veri ifadesi, bir kişinin fiziksel ve zihinsel sağlığının bütün yönleriyle ilgili bilgileri kapsayacak şekilde geniş yorumlanmalıdır"[33]. Görüldüğü üzere ATAD, Bayan *Lindqvist*'in ismi belli bir meslekdaşmın ayağını incittiğine ve bu nedenle de kısmi statüde çalıştığına ilişkin bilgileri internet sitesine koymasını Veri Koruma Direktifinin 8. maddesinin 1. fıkrası kapsamında saymıştır.

II. HASSAS VERİLERİN İŞLENEBİLECEĞİ HALLER

A. Genel Olarak

Hassas verilerin işlenmesi kural olarak yasaktır. Bu doğrultuda Veri Koruma Direktifi'nin 8. maddesinde sayılan hassas veriler için "kural olarak" işleme yasağı getirilmiştir (*prohibition to process sensitive data*). O halde hassas veriler ancak "istisnai olarak" işlenebilir. İşte Direktif de bazı hallerde hassas verilerin işlenmesine izin vermektedir. Bunlara hassas verilerin işlenebileceği istisnai haller adı verilir. Ancak burada şu husus da unutulmamalıdır ki hassas verilerin işlenebileceği istisnai haller, bu verileri Direktifin sağladığı korumadan yoksun bırakmamakta ancak aynı Direktifin 8. maddesinin sağladığı "özel koruma"dan yoksun bırakmaktadır. Örneğin, veri sahibinin açık muvafakatı Direktifin diğer korumalarıyla uyum içinde olma ihtiyacını ortadan kaldırmamakta, sadece Direktifin 8. maddesinin 1. fıkrasında yer alan işleme yasağını ortadan kaldırmaktadır[34].

---

[29] Aynı yerde para. 87. Nakleden **Macdonald/Crail/Jones**, s. 355; **Singleton**, 568-569.

[30] C-101/01, OJ C 7, 10.01.2004, p. 3.

[31] Para. 13.

[32] Para. 14.

[33] Para. 50.

[34] Dammann ve Simitis, s. 166. Nakleden **Kuner**, Christopher, European Data Protection Law: Corporate Compliance and Regulation, Second Edition, Oxford University Press, Oxford 2007, s. 101.

Veri Koruma Direktifinde, hassas verilerin istisnai hallerde işlenmesinin sıkı şekilde kontrol altına alınmasının önemi vurgulanmaktadır[35]. Veri koruma hukukunda geçerli olan hassaslık ilkesi (*the principle of sensitivity*), hassas verilerin (*sensitive personal data*) işlenmesinin sıradan verilerin (*ordinary personal data*) işlenmesinden daha katı denetime tabi tutulması anlamına gelmektedir[36]. Çünkü birçok veri sahibi, hassas verilerinin sınırlı şekilde işlenmesinden ve bu işlemenin kontrol altında bulunmasından emin olmak istemektedir. Yine veri koruma hukukunda geçerli olan "minimumluk ilkesi" (*principle of minimality*) hassas verilerin işlenmesinde dikkate alınması gereken bir sınırlama sebebidir. Çünkü "minimumluk ilkesi" (*principle of minimality*) toplanan kişisel veri miktarının, verilerin toplanması ve daha sonra işlenmesi amaçlarını başarmak için zorunlu olan miktarla sınırlı kalınmasını gerekli kılar[37]. Bu ilke açık şekilde Veri Koruma Direktifinin 6. maddesinin 1. fıkrasının c bendinde "aşırı olmama" (*not excessive*) kalıbı ile karşımıza çıkmaktadır. Aynı zamanda bu ilke Direktifin, kişisel verilerin ve hassas kişisel verilerin bir veya birden fazla şartın yerine gelmesi halinde işlenmesine izin veren 7 ve 8. maddelerinde de görülmektedir. Dolayısıyla "minimumluk ilkesi"nin hassas verilerin işlenmesinde dikkate alınması gereken bir sınırlama sebebi olduğu unutulmamalıdır.

Veri işlemenin diğer bütün gereklilikleri hassas veriler bağlamında daha katı ele alınır. Örneğin, Avrupa Mahkemeleri ve veri koruma otoriteleri, hassas verileri işleyen şirketlerin, işlemenin amaçları hakkında veri sahiplerini ayrıntılı olarak bilgilendirmelerini aramada özellikle katı davranmaktadır. Bu ilave yükümlülükler nedeniyle şirketlere neyin mutlak şekilde zorunlu olduğu konusunda hassas verileri işlemede sınırlar bildirilir. Çoğu zaman bir şirket, dikkatli inceleme sonucunda, gerçekten hassas verileri işlemenin gerekli olmadığını fark edebilir[38].

108 sayılı Sözleşme'de, ulusal hukuk uygun güvenceler (*appropriate safeguards*) getirmedikçe hassas verilerin otomatik olarak işlenemeyeceği hüküm altına alınmıştır[39]. 2000 tarihli Hollanda Veri Koruma Kanunu'nda hassas verilerin işlenebileceği haller ise her bir hassas veri için ayrı maddelerde düzenlenmiş (m. 17-22) ve bunlar dışında tek bir maddede de bütün hassas veriler için geçerli olan işleme halleri belirtilmiştir (m. 23)[40]. Bazı ülkelerin mevzuatı hassas verilerin işlenmesinden önce Ulusal Veri Koruma Otoritesi'nden izin alınmasını gerekli kılmaktadır. Örneğin, Danimarka Kişisel Verilerin Korunması Kanunu'nun 50. maddesinin 1. fıkrasına göre hassas verilerin işlenmesi bu konuda ön izin verecek olan Veri Koruma Otoritesi'ne bildirimi gerektirmektedir[41].

---

[35] Direktif, Recital 33.

[36] **Bygrave**, Lee A., Data Protection Law: Approaching Its Rationale, Logic and Limits, Kluwer Law International, The Hague 2002, s. 68.

[37] **Bygrave**, s. 341.

[38] **Kuner**, s. 102.

[39] 108 sayılı Sözleşme, m. 6.

[40] http://www.dutchdpa.nl/downloads_wetten/wbp.pdf (20.03.2010)

[41] http://www.datatilsynet.dk/english/the-act-on-processing-of-personal-data/ (20.03.2010)

Ulusal veri koruma otoriteleri bazı hassas veri türlerinin işlenmesi ile ilgili olarak rehber ilkeler de yayınlamıştır. Örneğin, Fransız Veri Koruma Otoritesi (CNIL), 8 Mart 2001 tarihinde sağlık alanında faaliyet gösteren internet siteleri hakkında bir tavsiye kararı yayınlamıştır[42]. Bu tavsiye kararı CNIL'm sağlıkla ilgili 60'm üzerinde internet sitesini denetlemesinin ve bu sitelerin sıklıkla veri koruma mevzuatının gereklerini yerine getirmediklerini tespit etmesinin sonucu olarak ortaya çıkmıştır. Tavsiye kararı şu ilkeleri getirmektedir[43]:

1) Belirli veya belirlenebilir bir kişiyle ilgili sağlık verisi, veri sahibi muvafakat gösterse bile satın alınamaz veya satılamaz.

2) Bireyler ziyaret ettiği zamanlarda sağlıkla ilgili internet siteleri tarafından toplanan gezgin (*navigational*) veriler, sağlıkla ilgili konular hakkında diğer verilerle birleştirilirse, hassas veri haline gelir. Örneğin, bir bireyin sağlıkla ilgili bir anket doldurması halinde olduğu gibi. Bu nedenle bu veriler sağlıkla ilgili veriler gibi işlem görmelidir. Tavsiye kararı aynı zamanda bu verilerin sigorta şirketlerine, bankalara ve işverenlere verilmesini yasaklamıştır.

3) Kamu otoriteleri, bu verilerin gizliliğini güvence altına almak amacıyla sağlıkla ilgili internet siteleri üzerinde sıkı denetimler gerçekleştirmelidir.

Bu açıklamalardan sonra Veri Koruma Direktifi uyarınca hassas verilerin işlenebileceği haller aşağıda sıralanmaktadır.

B. İşleme Halleri (İstisnalar)

1. Veri Sahibinin Açık Muvafakatı

Veri sahibinin (*the data subject*) açık muvafakatı (*explicit consent*) halinde hassas verileri işlenebilir. Zımni muvafakat Direktif tarafından kabul edilmemiştir. O halde hassas verilerin işlenebilmesi için veri sahibinin açık muvafakatı gerekmektedir. Bununla birlikte Veri Koruma Direktifi, üye ülkelere, veri sahibinin açık muvafakatı olsa bile hassas verilerin işlenmesini yasaklama imkanı getirmektedir[44]. Ancak, "devlet en iyisini bilir" (*the State knows best*) mantığından hareketle getirilen bu imkanın "kişisel verilerin kaderini tayin etme hakkına" (*iriformational self-determination*) aykırı olduğu ileri sürülmektedir[45].

"Açık" kavramı Direktifte tanımlanmamıştır. İngiltere'de Bilgi Görevlisi (*Iriformation Commissioner*) açık muvafakat konusunda şunları söylemektedir: "Veri sahibinin muvafakatı kesinlikle açık olmalıdır. Uygun durumlarda açık muvafakat, işlemenin spesifik detaylarını, işlenecek belirli veri çeşidini (spesifik bilgi dahil), işlemenin amaçlarını ve işlemenin bireyi etkileyebilecek özel yönlerini içermelidir"[46].

---

[42] Délibération No. 01-011 du 08 mars 2001 portant adoption d'une recommandation sur les sites de santé destinés au public.

[43] **Kuner**, s. 106-107.

[44] Direktif m. 8/2-a.

[45] **Korff**, Douwe, Data Protection Laws in the European Union, Direct Marketing Association, New York 2005, s. 45-46.

[45] Legal Guidance, s. 11. Nakleden **Jay**, s. 275-276; **Lloyd**, s. 103; **Carey**, s. 85; **Singleton**, 569.

Açık muvafakat, iradenin gönüllü, özgür, iradi ve bilinçli şekilde açıklanması ile ortaya çıkabilir. Ayrıca açık muvafakat veri sahibinin işleme hakkında yeterli ölçüde bilgilendirilmesini gerektirir. Aksi takdirde açık muvafakatın bulunduğu söylenemez[47]. Nihayet açık muvafakat belirli bir duruma ilişkin olmalıdır. Yani açık muvafakat, hassas verilerin işlenmesi için genel muvafakat (*general consent*) verilmesi anlamına gelmeyip belirli hassas verilerin işlenmesine ilişkin olarak verilen muvafakat anlamına gelmektedir[48].

Açık muvafakat, hassas verileri işleme amacının kapsamlı bir şekilde ortaya konması ve bunun yanında ilgili kişiye işaret veya imza kutucuğu yoluyla işlemeye muvafakatını gösterme imkanının tanınması yoluyla elde edilebilir[49]. Çünkü açık muvafakatın özü, veri sahibinin olumlu olarak (*positively*) muvafakatını göstermesine dayanmaktadır. Örneğin veri sahibi bu iradesini bir internet sitesinde bulunan kutucuğu "katılmayı tercih ediyorum" (*opt-in consent*) şeklinde işaretleyerek gösterebilir[50]. Tabi bu yolla muvafakat elde etmenin kabul edilebilir tarzı, veri sahibinin imzalayacağı ya da işaretleyeceği forma düşünülen işleme faaliyetini ya da faaliyetlerini tanımlayan bir ifadenin eklenmiş olmasıdır[51]. Yine bunun gibi bir iş müracaatında bulunan bir kişinin hassas veri içeren özgeçmişini sunması halinde açık muvafakatı var demektir[52].

Açık muvafakat, muvafakatın mutlaka yazılı olması gerektiği anlamına gelmemektedir. Fakat yazılı muvafakatın aranması ispat açısından faydalıdır. Bu itibarla yazılı muvafakat veri işleyenler (*the controller*) için daima bir güvence ve rahatlık sağlar[53].

2. Çalışma Hukuku Yükümlülüklerine Uyma

Yeterli güvenceler (*adequate safeguards*) sağlayan ulusal hukuk tarafından yetki verildiği sürece, veri işleyenin çalışma hukuku alanında yükümlülüklerini ve belli haklarını yerine getirme amacı için zorunlu ise hassas veriler işlenebilir[54]. Gerçekten de ulusal hukuk uyarınca veri işleyene görev olarak verilen hukuki bir yükümlülüğe uymak için hassas verileri işlemenin zorunlu olduğu durumlar bulunabilir. O nedenle bu istisna ulusal mevzuatın veri işleme konusunda işverenler üzerine açık bir hukuki yükümlülük getirmesi halinde uygulanabilir. Yalnız burada çalışma hukukunu salt iş hukuku alanına özgülememek kamu hukuku çalışma alanını da kapsayacak şekilde düşünmek gereklidir.

---

[47] **Carey**, s. 84-85.

[48] **Legal Essentials: Data Protection**, Hammond Suddards Edge, Chartered Institute of Personnel and Development, London 2000, s. viii.

[49] **Carey**, s. 85.

[50] **Room**, Stewart, Data Protection and Compliance in Context, BCS, Swindon 2007, s. 127; **Kuner**, s. 102.

[51] **Bainbridge**, David, Data Protection, Second Edition, xpl publishing, St Albans 2005, s. 99.

[52] **Legal Essentials: Data Protection**, s. viii.

[53] **Room**, s. 127; **Carey**, s. 85; **Jay**, s. 275.

[54] Direktif m. 8/2-b.

Çalışma hukuku ile ilgili verilerin işlenmesi açısından Direktif "yeterli güvenceler" şartını aramaktadır. Dikkat edileceği üzere burada veri sahibinin mutlaka veri işleyenin çalışanı olması gerekli değildir[55]. Çalışma hukuku ile ilgili olarak hassas verileri işleme yükümlülüğü bulunan pek çok durum bulunmaktadır. Örneğin İngiltere'de, mevzuat uyarınca işverenlerin iş yerinde meydana gelen kazaları kaydetme yükümlülüğü bunmaktadır. Bunun gibi işverenlerin işten çıkarmaları, sendika üyelik aidatı kesintisi kesme ve bunu sendikaya aktarmayı, işyerinin devrini, vergi ödemelerini, özürlü ayrımcılığını önlemek için istihdam ettiği özürlü çalışanları, cinsel eğilim ayrımcılığını önlemek için gay ve lezbiyen çalışanlar ile ilgili bilgileri kaydetme yükümlülüğü bulunmaktadır[56].

3. Veri Sahibinin Hayati Çıkarları

Veri sahibinin "fiziki" ya da "hukuki" nedenlerle muvafakatını veremeyeceği durumlarda, veri sahibinin veya diğer bir kişinin hayati çıkarlarını korumak için zorunlu ise hassas veriler işlenebilir[57]. Bu istisna esas itibarıyla insan yaşamını tehdit eden durumların varlığı halinde hassas verilerin işlenmesini amaçlamaktadır[58].

Fiili nedenlerle veri sahibinin muvafakatını veremeyeceği hallere veri sahibinin, geçirdiği bir kaza sonucunda kan nakli yapılmasına gerek duyulan bilinci kapalı bir kişi olması örneği verilebilir. Hukuki nedenlerle veri sahibinin muvafakatını veremeyeceği hallere ise veri sahibinin küçük ya da akli melekeleri yerinde olmayan bir kişi olması örneği verilebilir[59].

Dikkat edileceği üzere bu istisna hassas verilerin sadece "veri sahibi" hakkında değil aynı zamanda "diğer bir kişi" hakkında da işlenebilmesine imkan tanımaktadır. Bu durumda örneğin, veri sahibinin ciddi bir bulaşıcı hastalığı bulunması halinde veri sahibi ile irtibat halinde olabilecek kişilerin hayati çıkarlarını korumak amacıyla sağlık görevlileri, veri sahibinin muvafakatını almaksızın onunla ilgili hassas verileri işleyebilecektir. Diğer taraftan burada "diğer bir kişi" ibaresinin belli bir kişiyi mi, geniş anlamda toplum üyelerini mi yoksa belli bir grubu mu kastettiği konusunda açıklık bulunmadığı iddia edilmiştir[60]. *Jay*, zihinsel sağlık problemleri veya bulaşıcı ve ölümcül hastalıklar gibi veri sahibinin diğerlerinin hayati çıkarlarını tehdit ettiği hallerde bu ayrımın önemli olduğunu ifade etmektedir. Çünkü böyle bir durumda belli bir kişiye tehdidi göstermek zorunlu olacak mıdır yoksa topluma genel bir tehdidi göstermek yeterli olacak mıdır?[61] Bu örnekte tehdidin topluma yönelmesinin zorunlu olması aranmalıdır[62].

---

[55] Aynı yönde bkz. **Room**, s. 128.

[56] **Room**, s. 128; **Kuner**, s. 102.

[57] Direktif m. 8/2-c.

[58] **Bainbridge**, Data Protection, s. 100; **Singleton**, 571.

[59] **Bainbridge**, David, EC Data Protection Directive, Butterworths, London 1996, s. 56.

[60] **Jay**, s. 277.

[61] **Jay**, s. 277-278.

[62] Aynı yönde bkz. **Jay**, s. 278.

Bu istisna daha çok sağlıkla ilgili bilgiler hakkında uygulanabilir gözükse de diğer hassas verileri de ilgilendirmektedir. Örneğin, ırksal köken eğer bazı sağlık durumları veya hastalıklara yatkınlığı ortaya çıkarırsa veri sahibinin hayati çıkarları ile ilgili olabilir. Cinsel yaşam bazı hastalıklara yakalanmayı belirleme veya bazı hastalıkların nedenleri ile ilgili olabilir. Suç ve mahkumiyetler ile ilgili bilgiler hayati çıkarlarını korumak için bazı kişilere açıklanabilir. Dini inançlar, kan nakli örneğinde olduğu gibi bazı tıbbi tedavi türlerinin kabul edilebilirliği ile ilgili olabilir[63].

Veri sahibinin hayati çıkarları istisnası, İngiltere Veri Koruma Kanunu'nda[64] üç ihtimal dahilinde ayrıntılı olarak düzenlenmiştir. Buna göre,

1) Veri işleme, muvafakatın veri sahibi veya onun adına hareket eden kişi tarafından verilememesi halinde, veri sahibinin veya diğer bir kişinin hayati çıkarlarını korumak için zorunludur. Örneğin, veri sahibinin bilincinin kapalı (komada) olması[65] veya bulunamaması[66].

2) Veri işleme, veri işleyenin veri sahibinin muvafakatını elde etmesinin mantıken beklenmemesi halinde, veri sahibinin veya diğer bir kişinin hayati çıkarlarını korumak için zorunludur. Örneğin, veri sahibinin bulaşıcı bir hastalığın taşıyıcısı olması ve verinin bir üçüncü kişinin tedavisinde gerekli olması[67].

3) Veri işleme, muvafakatın veri sahibi veya onun adına hareket eden kişi tarafından mantığa aykırı olarak verilmesinden kaçınılması halinde, diğer bir kişinin hayati çıkarlarını korumak için zorunludur (Ek Cetvel 3/3). Örneğin, veri sahibinin bir akrabasının ciddi şekilde hasta olması halinde veri sahibinin sağlık geçmişinin tedavide önem arz ettiği bir durumda veri sahibinin bu verilerinin işlenmesinden kaçınması[68]; bulaşıcı bir hastalığa yakalanan veri sahibinin kendisiyle ilişki kurduğu kişileri –ki tedavi görmeleri için kendileriyle irtibat kurulması gerekebilir– açıklamaya rıza göstermekten kaçınması[69].

4. Özel Hukuk Tüzel Kişilerinin Faaliyetleri

Hassas veriler, uygun güvencelerle, siyasi, felsefi, dini veya sendikal amaç taşıyan bir vakfın, derneğin ve benzeri diğer kar amacı gütmeyen kuruluşların meşru faaliyetleri sırasında işlenebilir. Ancak bu durumda veri işlemenin sadece bu kuruluşların üyeleri veya amaçları için bu kuruluşlarla düzenli irtibat halinde olan kişiler hakkında olması ve verilerin, veri sahiplerinin muvafakatı olmaksızın üçüncü kişilere açıklanmaması şartı aranır[70]. Amaçları için bu kuruluşlarla düzenli irtibat halinde olan kişilere, bu kuruluşlara dü-

---

[63] **Jay**, s. 280.

[64] İngiltere Veri Koruma Kanunu'nun gelişimi konusunda bkz. **Bennett**, Colin J., Regulating Privacy: Data Protection and Public Policy in Europe and the United States, Cornell University Press, New York 1992, s. 82 vd.

[65] **Lloyd**, s. 103; **Bainbridge**, Data Protection, s. 100; **Jay**, s. 278.

[66] **Carey**, s. 86.

[67] **Lloyd**, s. 103; **Carey**, s. 86.

[68] **Bainbridge**, Data Protection, s. 100.

[69] **Lloyd**, s. 104.

[70] Direktif m. 8/2-d.

zenli olarak yardımda bulunan kişiler örnek gösterilebilir[71]. Veri Koruma Direktifinde bu kuruluşların hassas verileri işlemelerinde kilit noktanın "kamu yararı" (*public interest*) olduğu ifade edilmiştir[72].

Görüldüğü gibi bu istisna kar amacı gütmeyen bazı kuruluşlara faaliyet alanları ile ilgili hassas verileri işleme konusunda izin vermektedir. Dikkat edileceği üzere bu istisna kar amacı gütmeyen bütün kuruluşlar için değil sadece siyasi, felsefi, dini veya sendikal amaçlı kar amacı gütmeyen kuruluşlar için uygulanacaktır. Örneğin bu istisna, belli etnik grupları desteklese yahut tıp ya da cinsellik alanında faaliyet gösterse bile ticari amaç güden kuruluşları kapsamayacaktır[73].

Bu istisnanın uygulanmasında birtakım zorluklar da bulunmaktadır. Şöyle ki siyasi, felsefi, dini veya sendikal amaç taşıyan vakıflar, dernekler ve benzeri diğer kar amacı gütmeyen kuruluşlar bugün ya doğrudan doğruya kendileri yarı ticari nitelikte faaliyetlerde bulunmakta ya da kar amacı güden kuruluşlarla işbirliği içinde olmaktadır. Dolayısıyla böyle bir durumda nasıl hareket edileceği belirsizdir[74].

5. Verilerin Kamuya Açıklanmış Olması

Veri sahibi tarafından açık şekilde (*manifestly*)[75] kamuya açıklanan hassas veriler işlenebilir[76]. Bu istisna veri sahibinin hassas verilerini iradi olarak (*self-explanatory*) kamuya açıklanması haline ilişkindir. Diğer bir ifadeyle, hassas veri içeren bilgiler veri sahibinin iradesiyle kamuya açıklanmışsa/kamu malı haline gelmişse (*iriformation in the public domain*) artık işlenmeleri mümkündür. Ancak verilerin salt kamuya açıklanması yeterli olmayıp bu açıklamanın veri sahibinin iradesiyle gerçekleşmesi gerekmektedir. Bu duruma örnek olarak bir televizyon programında veri sahibinin HIV virüsü taşıyıcısı olduğunu söylemesini gösterebiliriz.

Tabi burada asıl zorluk "açık şekilde" ve "kamuya açıklama" kavramlarının ne anlama geldiğini tespit noktasında karşımıza çıkmaktadır[77]. Bir televizyon programında hassas verileri ile ilgili konuşan veri sahibinin bu verileri açıkça kamuya açıkladığı söylenebilirken aynı kişinin bu konuşmayı bir arkadaş ortamında ya da evde eşine yapmasında durum değişecektir[78]. Bunun gibi bir lokantada yemek yerken sinirlerine hakim olamayan bir kişinin bu esnada bazı hassas verilerini açıklaması halinde durum ne olacaktır?[79] Dolayısıyla,

---

[71] **Bainbridge**, Data Protection, s. 101.

[72] Direktif, Recital 33, 35 ve 36.

[73] **Korff**, s. 47.

[74] **Korff**, s. 47.

[75] İngiltere Veri Koruma Kanunu'nda "açık şekilde" ibaresi yerine "kasden" (*deliberately*) ibaresi kullanılmıştır.

[76] Direktif m. 8/2-e.

[77] Benzer endişeler için bkz. **Jay**, s. 280-281; **Carey**, s. 86.

[78] **Carey**, s. 86; **Jay**, s. 280-281.

[79] **Jay**, s. 281.

hassas verilerin işlenmesine imkan tanıyan bu istisnanın her somut olayda ayrı ayrı değerlendirilmesi gerekmektedir.

Avrupa İnsan Hakları Mahkemesi, *Von Hannover v. Germany* davasında özel bir akşam yemeğinde Monako Prensesi Caroline'in fotoğraflarının çekilmesini, yemek kamuya açık bir yerde yenmesine rağmen, Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesinin ihlali olarak görmüştür[80].

Bu istisna sadece bilgilerin kamuya açıklanması hali ile sınırlı olarak mı uygulanacaktır? Çünkü hassas veriler, bir kişinin etnik kökeni, başını örten bir Sikh'in dini inançları ya da bir kişinin özür durumu örneklerinde olduğu gibi görsel olarak da kamuya açıklanabilir. O halde görsellik halinin bilgileri kamuya açıklama sayılıp sayılmayacağı ile ilgili bir soru sorulabilir. Yani hukuk özürlü olduğunu kamuya açıklayan bir kişi ile görünürde özürlü olan bir kişi arasında gerçekten bir ayrım yapmak istemekte midir?[81].

6. Hukuki İddiaları Tesis Etme Uygulama ve Savunma

Hukuki iddiaları tesis etme, uygulama ve savunma için zorunlu ise hassas veriler işlenebilir[82]. Avukatların, müvekkillerinin talimatlarını yerine getirirken yaptığı birçok faaliyet bu istisna kapsamında yer alır[83]. Yine bu istisna veri işleyenlere hassas verileri hukukçularına açıklama hakkı verir. Halihazırda çalışan bir işçi veya eski bir işçi tarafından bir ayrımcılık davası açılması üzerine veya işyerinde meydana gelen bir kaza üzerine veri işleyen hukuki tavsiye (yardım) alma gereği duyacaktır. Bu istisna hem işverenleri hem de onlara yardım eden hukuk görevlilerini korur[84].

7. Sağlık Gerekleri

Önleyici tıp (*preventative medicine*)[85], tıbbi teşhis ve tanı, bakım ve tedavi sunma, sağlık hizmetlerinin yönetimi amaçları için zorunlu ise hassas veriler işlenebilir[86]. Ancak bu hallerde veriler, ulusal hukuka veya mesleki gizlilik yükümlülüğü ile ilgili ulusal yetkili kurumlar tarafından geliştirilen kurallara tabi sağlık görevlileri ya da aynı (eşdeğer) düzeyde gizlilik yükümlülüğü bulunan diğer kişiler tarafından işlenebilir[87]. Sağlık görevlisi kavramının içerisine doktorlar, hemşireler, ebeler, dişçiler, gözlükçüler, eczacılar ve diğerleri girer.

---

[80] Application No: 59320/00, 24 Eylül 2004.

[81] **Jay**, s. 281.

[82] Direktif m. 8/2-e.

[83] **Carey**, s. 87.

[84] **Room**, s. 131.

[85] Önleyici tıp, hastalıkları önleme ile ilgili bir tıp dalı olup hastalıkları tedavi etmekten ziyade onları önlemek için alınacak tedbirlerle ilgilenir. Göğüs ya da prostat kanseri gibi hastalığı önleyici testler buna örnek verilebilir.

[86] Direktifte tıbbi araştırmalar (*medical research*) sayılmamıştır.

[87] Direktif m. 8/3.

8. Suçlar Mahkumiyetler ve Güvenlik Tedbirleri

Suçlar, mahkumiyetler ve güvenlik tedbirleri[88] ile ilgili veriler ancak resmi bir makam tarafından işlenebilir[89]. Bu veriler suçu işlediğinden şüphelenilen kişiler ya da daha az cezayı gerektiren suçları işleyen kişilere yapılan uyarılar hakkındaki bilgileri de içerebilir[90]. Veri Koruma Direktifi uygun güvenceler altında bu kurala istisna getirilmesine imkan tanımaktadır[91]. Ancak bu istisnanın uygulanması halinde durum Komisyona da bildirilmelidir[92]. Bu durumda örneğin, mahkumiyetler hakkındaki bilgiler, banka ve sigorta şirketleri gibi potansiyel sahtekarlıkları ortaya çıkarma amaçlı kurumlar tarafından işlenebilir. Bir sigorta şirketinin, yangın nedeniyle doğan zararı talep eden sigortalısının daha önce yangın çıkarma (*arson*) suçundan mahkum olduğunu bilmesi özellikle kişinin bu bilgiyi açıklamaması halinde, yararına olacaktır[93].

Ancak adli sicil kayıtları (*a complete register of criminal convictions*) ise ancak resmi bir makam tarafından işlenebilir[94]. Bu konuda bir istisna getirilemez. Diğer taraftan bu zorunluluk, suçlar ve güvenlik tedbirlerini içerecek şekilde de genişletilemez.

Nihayet AB Veri Koruma Direktifi üye ülkelere, isteğe bağlı olarak, idari yaptırımlar ve adli mahkemeler tarafından verilen kararlar ile ilgili verilerin resmi makamlar tarafından işlenebileceği yönünde düzenleme yapabilmelerine imkan tanımaktadır[95]. Direktif, bu nitelikteki verilerin resmi bir makam dışında özel hukuk kişileri tarafından da işlenmesine izin vermektedir. Bu doğrultuda, borç veya diğer tür kredi veren kurumlar, örneğin, borçlular aleyhine verilen adli mahkeme kararlarını işleyebilmelidir. Bu durum kurumların meşru çıkarları için zorunludur. Aksi takdirde bu kurumlar borçlarını ödememe kaydı bulunan kişilere karşı zayıf konumda bulunacaklardır[96].

9. Ulusal Kimlik Numarası

Direktifte ulusal kimlik numarası ile diğer tanıtıcı işaretlerin işlenme şartlarını belirleme konusunda üye ülkelere yetki verilmektedir. Bu hüküm üye ülkelere getirecekleri şartları belirleme konusunda oldukça geniş bir takdir yetkisi vermektedir[97].

---

[88] Güvenlik tedbirleri kavramı IT güvenliğini değil şartlı salıverme ve ev hapsi gibi ceza hukuku tedbirlerini ifade eder. **Kuner**, s. 101.

[89] Direktif m. 8/5.

[90] **Bainbridge**, EC Data Protection Directive, s. 57.

[91] Direktif m. 8/5.

[92] Direktif m. 8/6.

[93] **Bainbridge**, EC Data Protection Directive, s. 57.

[94] Direktif m. 8/5.

[95] Direktif m. 8/5.

[96] **Bainbridge**, EC Data Protection Directive, s. 57.

[97] Direktif m. 8/7.

C. Ek İşleme Halleri (Ek İstisnalar)

Veri Koruma Direktifinde hassas verileri işleme konusunda esneklik sağlama düşüncesiyle üye ülkelere ek istisnalar getirebilme imkanı tanınmıştır. Direktife göre üye ülkeler, uygun güvenceler öngörmek suretiyle, "önemli/ üstün kamu yararı gerekçesiyle" (*for reasons of substantial public interest*) ulusal hukuk yoluyla ya da veri koruma otoritesinin kararıyla yukarıda sayılanlara ek istisnalar getirebilir[98]. Ancak üye ülkeler tarafından getirilecek olan bu ek istisnaların Komisyona bildirilmesi gerekmektedir[99].

Hassas verilerin işlenebileceği 20 istisna kabul eden İngiltere, bunların 9'unu Veri Koruma Kanunu ile, 10'unu 2000 tarihli Veri Koruma (Hassas Kişisel Verilerin İşlenmesi) Emri[100] ile ve 1'ini de 2002 tarihli Veri Koruma (Hassas Kişisel Verilerin İşlenmesi) (Seçilmiş Temsilciler) Emri ile getirmiştir. İngiltere Veri Koruma Kanunu'na Ek Cetvel 3'te farklı ırki ve etnik kökene sahip insanlar arasında fırsat eşitliğini sağlamak için zorunlu ise hassas verilerin işlenebileceği kabul edilmektedir. 2000 tarihli Veri Koruma (Hassas Kişisel Verilerin İşlenmesi) Emri'nde, hukuka aykırı bir hareketi önleme veya ortaya çıkarma amacı için zorunlu ise[101]; kamunun korunması için zorunlu ise[102] hassas verilerin işlenmesine izin verilmektedir. 2002 tarihli Veri Koruma (Hassas Kişisel Verilerin İşlenmesi) (Seçilmiş Temsilciler) Emri, milletvekilleri ve diğer seçilmiş temsilcilerin, kendi faaliyetlerini yürütmek amacıyla hassas verileri işleyebileceğini öngörmektedir[103].

SONUÇ

Hassas veriler konusu oldukça önemli, nazik ve zor bir konudur. Veri Koruma Direktifinde hassas verilerin ayrı bir madde halinde düzenlenmesi ve farklı bir statüye tabi tutulması herhalde konunun önemini göstermek için yeterli bir delildir. İşin en başında hangi tür verilerin hassas veri olarak kabul edileceği hususunda veri koruma kanunlarında farklı düzenlemeler mevcuttur. Hatta kanun koyucunun hassas veri algılaması ile bireylerin hassas veri algılamasında da farklılıklar bulunmaktadır. Veri koruma kanunlarında hassas verilerin nelerden ibaret olduğunu saymak yeterli olmamakta, somut örneklerle karşılaşıldığında durum içinde çıkılamaz hal alabilmektedir. Bu noktada da mahkemelere büyük görevler düşmektedir. Bilim ve teknolojinin ilerlemesi sonucunda biometriklerin kullanımının artması ve DNA veritabanları gibi gelişmeler bizleri hassas veri türlerini yeniden gözden geçirmeye zorlamaktadır.

---

[98] Direktif m. 8/4.

[99] Direktif m. 8/6.

[100] The Data Protection (Processing of Sensitive Personal Data) Order 2000. SI 2000/417. Nakleden **Lloyd**, s. 105; **Carey**, s. 82; **Jay**, s. 286; **Room**, s. 41, 133; **Singleton**, 572.

[101] **Bainbridge**, Data Protection, s. 51, 97, 104-105; **Carey**, s. 88; **Jay**, s. 286; **Room**, s. 41, 134-135.

[102] **Carey**, s. 89; **Jay**, s. 286; **Room**, s. 135.

[103] The Data Protection (Processing of Sensitive Personal Data) (Elected Representatives) Order 2000. SI 2002/2905. Nakleden **Lloyd**, s. 107; **Bainbridge**, Data Protection, s. 106; **Carey**, s. 92-93; **Jay**, s. 291-292; **Room**, s. 140.

Hassas verileri işleme olayın bir diğer zor yönüdür. Bu konuda kural hassas verileri işleme yasağıdır. Ancak bu yasak hem Veri Koruma Direktifinde hem de veri koruma kanunlarında mutlak olarak uygulanmamaktadır. Çünkü bu düzenlemelerde hassas verilerin işlenmesinde hukuka uygunluk halleri öngörülmüştür. Bu yolla hassas verilerin işlenmesi yasağına nitelikli sınırlar çizilmeye çalışılmıştır. Hassas verilerin işlenebileceği haller konusunda da veri koruma kanunlarında farklı düzenlemeler mevcuttur. Burada bir husus daha önem arz etmektedir. Hassas verilerin işlenebileceği haller mutlaka kanunda belirtilmelidir. Bu noktada İngiltere örneği eleştirilebilir. Ayrıca hassas verilerin işlenebileceği hallerde, mümkün olan durumlarda, zorunluluk şartı (*the necessity criterion*) aranmalıdır. Nihayet, hassas veri işleyenler somut olaya en uygun istisnaya dayanmalıdır.

KAYNAKLAR

Bainbridge, David, EC Data Protection Directive, Butterworths, London 1996.

Bainbridge, David, Data Protection, Second Edition, xpl publishing, St Albans 2005.

Bennett, Colin J., Regulating Privacy: Data Protection and Public Policy in Europe and the United States, Cornell University Press, New York 1992.

Bygrave, Lee A., Data Protection Law: Approaching Its Rationale, Logic and Limits, Kluwer Law International, The Hague 2002.

Carey, Peter, Data Protection: A Practical Guide to UK and EU Law, Third Edition, Oxford University Pres, Oxford 2009.

Jay, Rosemary, Data Protection: Law and Practice, Sweet & Maxwell, London 2007.

Korff, Douwe, Data Protection Laws in the European Union, Direct Marketing Association, New York 2005.

Kuner, Christopher, European Data Protection Law: Corporate Compliance and Regulation, Second Edition, Oxford University Press, Oxford 2007.

Legal Essentials: Data Protection, Hammond Suddards Edge, Chartered Institute of Personnel and Development, London 2000.

Lloyd, Ian J., Information Technology Law, Fifth Edition, Oxford University Press, Oxford 2008.

Macdonald, John / **Crail**, Ross / **Jones** Clive H., The Law of Freedom of Information, Second Edition, Oxford University Press, Oxfod 2009.

Room, Stewart, Data Protection and Compliance in Context, BCS, Swindon 2007.

Schwartz, Paul M. / **Reidenberg**, Joel R., Data Privacy Law: A Study of United States Data Protection, Michie Law Publishers, Virginia 1996.

Singleton, Susan, Tolley's Data Protection Handbook, 4th Edition, Lexis NexisButterworths, London 2006.